

ATTACHMENT A

I. DESCRIPTION OF PROPERTY TO BE SEARCHED

1. This warrant applies to information associated with the Google, Inc. e-mail account of **1234wjwj@gmail.com**, controlled by the web-based electronic communication service provider known as Google, Inc., headquartered at 600 Amphitheater Parkway, Mountain View, CA 94043.

II. SERVICE OF WARRANT AND SEARCH PROCEDURE

1. The officer executing this warrant shall affect service by any lawful method, including faxing the warrant to the location specified in the warrant.
2. To minimize any disruption of computer service to third parties, the officer executing this warrant shall direct the service provider's employees to locate, isolate, and create an exact duplicate of all contents of communications, records, and other information associated with the subscriber account(s) as described in Section III below.
3. The terms "records," "information," "communications," "contents," and "files" include all of the items described in this Attachment in whatever form and by whatever means they may have been created or stored, including, without limitation, any electronic or magnetic form (such as hard drives, floppy disks, CD-ROMs, backup tapes, and printouts or readouts from any such media), and any handmade, mechanical, or photographic form (such as writing, printing, typing, or photocopies).
4. The service provider's employees will provide the exact duplicate in electronic form (or as printouts if the original records are not in electronic form) of the subscriber account files described in Section III below to the agent who serves this search warrant, who need not be present at the location specified in the warrant during the retrieval of records, as permitted in 18 U.S.C. § 2703(g).
5. Law enforcement personnel will thereafter review the information stored in the files and accounts received from the service provider and then identify the relevant communications, records, and information contained in the files as described in Section IV below.

III. FILES AND ACCOUNTS TO BE COPIED BY EMPLOYEES

1. All electronic mail and electronic data stored and presently contained in, or on behalf of, the following account – **1234wjwj@gmail.com** (hereafter "the subject account") – and any and all other aliases or screen names associated with this account.

2. All existing printouts from original storage of all of the electronic mail described above in Section III (1).
3. All transactional information of all activity of the electronic mail addresses and/or individual accounts described above in Section III (1), including log files, dates, times, methods of connecting ports, dial-ups, and/or locations.
4. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above in Section III (1), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, passwords, and detailed billing records.
5. All records indicating the services available to subscribers of the electronic mail addresses and/or individual accounts described above in Section III (1).
6. All instant messages stored and presently contained in, or on behalf of, the subject account, and any and all other aliases or screen names associated with this account.
7. Copies of all images, videos, or graphics posted to the service provider's properties, photos, briefcase, or otherwise stored and/or associated with the subject account or any other screen names/email addresses associated with the subject account.

IV. INFORMATION TO BE REVIEWED AND IDENTIFIED BY LAW ENFORCEMENT PERSONNEL

1. Upon receipt of the information described in Section III above, law enforcement personnel will identify and copy the following information:

- a. From the communications, electronic data, records, and information described above in Section III, all electronic mail, clubs, web pages, or other communications and account contents, and all transactional and subscriber information from the subject account and any and all other aliases or screen names associated with this account, and e-mail sent to, from, or through such subscriber accounts, whether or not the electronic mail or account contents have been retrieved, that constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252, as well as all of the records and information described above in Section III (1-7) that constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252.

V. DELIVERY OF FILES BY GOOGLE INC. TO THE FEDERAL GOVERNMENT

1. Google Inc. shall disclose and deliver data responsive to the warrant, if any, by sending the data to Special Agent Jason Adams, Homeland Security Investigations, 3000 Sidney Street, Suite 300, Pittsburgh, PA 15203, via the United States Postal Service or commercial carrier.

ATTACHMENT B

DESCRIPTION OF PROPERTY TO BE SEARCHED

1. This warrant applies to information associated with the Google, Inc. e-mail account of **1234wjwt@gmail.com**, controlled by the web-based electronic communication service provider known as Google, Inc., headquartered at 600 Amphitheater Parkway, Mountain View, CA 94043.

II. SERVICE OF WARRANT AND SEARCH PROCEDURE

1. The officer executing this warrant shall affect service by any lawful method, including faxing the warrant to the location specified in the warrant.
2. To minimize any disruption of computer service to third parties, the officer executing this warrant shall direct the service provider's employees to locate, isolate, and create an exact duplicate of all contents of communications, records, and other information associated with the subscriber account(s) as described in Section III below.
3. The terms "records," "information," "communications," "contents," and "files" include all of the items described in this Attachment in whatever form and by whatever means they may have been created or stored, including, without limitation, any electronic or magnetic form (such as hard drives, floppy disks, CD-ROMs, backup tapes, and printouts or readouts from any such media), and any handmade, mechanical, or photographic form (such as writing, printing, typing, or photocopies).
4. The service provider's employees will provide the exact duplicate in electronic form (or as printouts if the original records are not in electronic form) of the subscriber account files described in Section III below to the agent who serves this search warrant, who need not be present at the location specified in the warrant during the retrieval of records, as permitted in 18 U.S.C. § 2703(g).
5. Law enforcement personnel will thereafter review the information stored in the files and accounts received from the service provider and then identify the relevant communications, records, and information contained in the files as described in Section IV below.

III. FILES AND ACCOUNTS TO BE COPIED BY EMPLOYEES

1. All electronic mail and electronic data stored and presently contained in, or on behalf of, the account **1234wjwt@gmail.com** (hereinafter "subject account") and any and all other aliases or screen names associated with this account.
2. All existing printouts from original storage of all of the electronic mail described above in Section III (1).

3. All transactional information of all activity of the electronic mail addresses and/or individual accounts described above in Section III (1), including log files, dates, times, methods of connecting ports, dial-ups, and/or locations.
4. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above in Section III (1), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, passwords, and detailed billing records.
5. All records indicating the services available to subscribers of the electronic mail addresses and/or individual accounts described above in Section III (1).
6. All instant messages stored and presently contained in, or on behalf of, the subject account, and any and all other aliases or screen names associated with this account.
7. Copies of all images, videos, or graphics posted to the service provider's properties, photos, briefcase, or otherwise stored and/or associated with the subject account or any other screen names/e-mail accounts associated with the subject account.

IV. INFORMATION TO BE REVIEWED AND IDENTIFIED BY LAW ENFORCEMENT PERSONNEL

1. Upon receipt of the information described in Section III above, law enforcement personnel will identify and copy the following information:
 - a. From the communications, electronic data, records, and information described above in Section III, all electronic mail, clubs, web pages, or other communications and account contents, and all transactional and subscriber information from the subject account and any and all other aliases or screen names associated with this account, and e-mail sent to, from, or through such subscriber accounts, whether or not the electronic mail or account contents have been retrieved, that constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt/distribution of a visual depiction of a minor engaged in sexually explicit conduct); and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct).